REMARKS

Examiner rejected claims 1-21 under 35 U.S.C. §103 as being unpatentable over Figs. 1 and 2 of Applicant's admitted prior art (AAPA) and in view of U.S. Pat. Appl. Pub. Nos. 20080043686 (Sperti et al.) and 20050213553 (Wang).

With regard to claims 1 and 2, Examiner said that the AAPA discloses a rogue access point and transmit channel preprocessor. It does not. The AAPA only discloses a rogue access point preprocessor and not a preprocessor concerning transmit channel as does Applicant. Applicant's RogueAPTransmitChannel preprocessor detects a channel on which a received packet is transmitted. The AAPA does not do this. Therefore, the AAPA does not disclose Applicant's RogueAPTransmitChannel preprocessor and, therefore, does not disclose Applicant's claim 1 or claim 2.

Examiner said that Sperti et al., in paras. 74 and 128, and Wang, in para. 35, disclose Applicant's preprocessors as follows: RogueClient, BridgedNetwork, RogueClientValidAP, ValidClientRogueAP, AdhocNetwork, WrongChannel, CloakingViolation, EncryptionViolation, and NullSSIDViolation.

Examiner citation to Sperti et al. in paragraph 128 lists a configuration list of valid APs, clients, and channels. None of these disclose Applicant's preprocessors.

Examiner's citation to Sperti et al. in paragraph 128 also mentions that "an alert is generated when information obtained from a packet does not match the information in the configuration file." Such a citation is a broad description that discloses the general operation of an Intrusion Detection System such as SNORT, which Applicant admitted is prior art. Applicant did not claim to have invented the general operation of an IDS. Instead, Applicant claimed to have improved an IDS by including preprocessors that previously did not exist. Examiner's citation does not disclose the new preprocessors that Applicant included in Applicant's patent application.

Applicant's RogueClient preprocessor detects a rogue client. Nowhere in Examiner's citations is a preprocessor disclosed to detect a rogue client. Therefore, neither Sperti et al. nor Wang disclose Applicant's RogueClient preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's BridgedNetwork preprocessor detects a wireless distribution system (or bridged network). Nowhere in Examiner's citations is a preprocessor disclosed to detect a wireless distribution system (or bridged network). Therefore, neither Sperti et al. nor Wang disclose Applicant's BridgedNetwork preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's RogueClientValidAP preprocessor detects an unauthorized client attempting to connect to a valid access point (AP). Nowhere in Examiner's citations is a preprocessor disclosed to detect an unauthorized client attempting to connect to a valid AP. Therefore, neither Sperti et al. nor Wang disclose Applicant's RogueClientValidAP preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's ValidClientRogueAP preprocessor detects an authorized client attempting to connect to a rogue AP. Nowhere in Examiner's citations is a preprocessor disclosed to detect an authorized client attempting to connect to a rogue AP. Therefore, neither Sperti et al. nor Wang disclose Applicant's ValidClientRogueAP preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's AdhocNetwork preprocessor detects beacons for an ad-hoc network, two devices in an ad-hoc network, and an authorized client in ad-hoc mode with a rogue client. Nowhere in Examiner's citations is a preprocessor disclosed to detect beacons for an ad-hoc network, two devices in an ad-hoc network, and an authorized client in ad-hoc mode with a rogue client. Examiner's citation to Sperti et al. in paragraph 74 also mentions "RF Jamming using ad-hoc networks." Using an ad-hoc network does not disclose Applicant's AdHocNetwork preprocessor, because using an ad-hoc network does not disclose detecting beacons for an ad-hoc network, two devices in an ad-hoc network, and an authorized client in ad-hoc mode with a rogue

client as does Applicant's AdHocNetwork preprocessor. Therefore, Examiner's citations do not disclose Applicant's AdHocNetwork preprocessor. Therefore, neither Sperti et al. nor Wang disclose Applicant's AdHocNetwork preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's WrongChannel preprocessor detects a device operating on an unauthorized channel. Nowhere in Examiner's citations is a preprocessor disclosed to detect a device operating on an unauthorized channel. Therefore, neither Sperti et al. nor Wang disclose Applicant's WrongChannel preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's CloakingViolation preprocessor detects when an SSID is not NULL when it should be NULL. Nowhere in Examiner's citations is a preprocessor disclosed to detect when an SSID is not NULL when it should be NULL. Therefore, neither Sperti et al. nor Wang disclose Applicant's CloakingViolation preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's EncryptionViolation preprocessor detects when a device is operating counter to an encryption policy (i.e., not using encryption when the policy requires encryption and using encryption when the policy requires no encryption). Nowhere in Examiner's citations is a preprocessor disclosed to detect when a device is operating counter to an encryption policy. Examiner's citation to Sperti et al. in paragraph 128 also mentions "authentication and encryption method." Examiner failed to put the citation in proper context. The actual citation is to "encryption and authentication method used." So, examiner's citation is to using an encryption method. Using an encryption method is not the same as detecting if a device is violating an encryption policy as does Applicant's EncryptionViolation preprocessor. Therefore, Examiner's citation does not disclose Applicant's EncryptionViolation preprocessor.
Therefore, neither Sperti et al. nor Wang disclose Applicant's EncryptionViolation preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Applicant's NullSSIDViolation preprocessor detects when a device attempts to associate with a client that sent a NULL SSID. Nowhere in Examiner's citations is a preprocessor disclosed to detect when a device attempts to associate with a client that sent a NULL SSID. Examiner said that Wang, in paragraph 35, discloses detecting attacks related to cloaking violations and NULL SSID. Examiner appears to quote Wang as disclosing "detecting attacks comprising a NULL/weak/default SSID probe request sent to an AP in an association or re-association request in an attempt to violate the cloaking policy of "cloaking or defaulting" the SSID of an AP." If this was intended to be a quote, it was mistakenly quoted, because the citation neven discloses the use of a NULL SSID. Instead, an SSID is checked to determine if it is weak or is a default SSID. Neither a weak nor a default SSID is a NULL SSID. Per the two attachment documents from About.com, a default SSID is a defined SSID set by the manufacturer of the device. A weak SSID implies that it is an SSID that is easily determined. A NULL SSID is no SSID, which is neither a defined SSID nor an easily determined SSID. In addition, Examiner's citation never mentions NULL. The Examiner inserted NULL himself. Examiner appears to have improperly used Applicant's application as the motivation to insert NULL into a citation that did not include NULL. Examiner committed error by doing so. Furthermore, Examiner associates "defaulting" with "cloaking". "Cloaking is the use of a NULL SSID, whereas "defaulting" is the setting of an SSID to a default value. "defaulting" is not equivalent to "cloaking." Therefore, Examiner committed error by associating the terms. Therefore, neither Sperti et al. nor Wang disclose Applicant's NULLSSIDViolation preprocessor and, therefore, do not disclose Applicant's claim 1 or claim 2.

Examiner said that it would be obvious to one of ordinary skill to modify the teachings of the AAPA to include preprocessors for detecting attacks taught by Sperti and Wang for the purpose of increased security by having a system that can detect as many attacks as possible. Examiner admits that Sperti et al. and Wang was not cited for disclosing Applicant's preprocessors but for disclosing attacks. An attack is not a preprocessor, because there may be many different solutions to an attack. A preprocessor is a specific solution to an attack.

The third step of claims 3 and 13 is if the frame does not contain a BSSID and is not an ACK then setting global variable Transmit_Channel equal to zero and returning to step (h) in claim 2. Nowhere in Examiner's citations is such a step disclosed.

The fourth step of claims 3 and 13 is if the frame contains a BSSID or is an ACK then determining if the packet is a beacon frame or a probe response. Nowhere in Examiner's citations is such a step disclosed.

The fifth step of claims 3 and 13 is if either frame type is identified then identifying the BSSID and the channel in its header. Nowhere in Examiner's citations is such a step disclosed.

The sixth step of claims 3 and 13 is determining if the BSSID is in a rogue AP list. Nowhere in Examiner's citations is such a step disclosed.

The seventh step of claims 3 and 13 is if the BSSID is not in the rogue AP list then determining if the BSSID is on a valid AP list. Nowhere in Examiner's citations is such a step disclosed.

The eighth step of claims 3 and 13 is if the BSSID is not on the valid AP list then adding the BSSID and its channel to the rogue AP list, setting global variable Transmit_Channel equal to the BSSID channel, and returning to step (h) in claim 2. Nowhere in Examiner's citations is such a step disclosed.

The ninth step of claims 3 and 13 is if the BSSID is in the rogue AP list or the BSSID is not in the rogue AP list but is in the valid AP list then updating the channel information in the corresponding rogue and valid AP list entry, setting global variable Transmit_Channel equal to the BSSID channel, and returning to step (h) in claim 2. Nowhere in Examiner's citations is such a step disclosed.

The tenth step of claims 3 and 13 is if the frame is neither a beacon frame nor a probe response then finding the BSSID in the header. Nowhere in Examiner's citations is such a step disclosed.

The eleventh step of claims 3 and 13 is determining if the BSSID or destination address is in a rogue AP list. Nowhere in Examiner's citations is such a step disclosed.